AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
Health Insurance Portability and Accountability Act (8/12/04)	Health Benefits Branch	2.1 CalPERS should ensure that its training program specifically identifies staff that require training, appropriate training to be provided, and ensure attendance at that training. Training documentation should demonstrate ongoing compliance with HIPAA requirements.	COMPLETE. Health Benefits Branch issued a memorandum to all Division Chiefs describing the federal regulations requiring training for all employees who work with or are exposed to HIPAA protected information. The training module is provided on HIPAA Administration's web site, and management will report completion of training to HIPAA Administration to enable documentation and tracking of the required training.
HIPAA Security Compliance Review (10/20/06)	Information Security Office	1.1 A thorough assessment has not been conducted of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of all Electronic Protected Health Information. The Information Security Office should conduct this assessment.	IN PROGRESS. The Information Security Office states that the risk analysis pilot program was completed in April 2008. Additionally it has produced risk assessment reports for the IT Infrastructure and Health Benefits Branch. The Information Security Office stated it had started the HIPAA risk assessment with plans of completion by ~~July 2008 August 2008~~ February 2009.
		1.2 CalPERS implements security measures to protect information assets housed at CalPERS to readily demonstrate HIPAA security compliance. Information Security Office should implement required security specifications and assess whether each addressable specification is a reasonable safeguard in the CalPERS environment based on risk analysis results.	IN PROGRESS. The Information Security Office states that this finding will be addressed as part of the IT infrastructure and Health Benefits Branch assessments. The Information Security Office plans completion of these assessments, which will include all identified data systems containing Electronic Personal Health Information, by ~~August 2008~~ February 2009.
		1.4 CalPERS' Event Logs Practice requires specific security events be logged at key servers. However, the practice does not specify which events must be logged at which system components, nor does it specify monitoring roles, responsibilities and frequency.	IN PROGRESS. The Information Security Office states that it plans to create a HIPAA Security Practice that identifies security requirements specifically for systems containing Electronic Protected Health Information. The Information Security Office states that the new practice will be drafted after the Health Benefits Branch risk assessment and plans to finalize the practice by ~~October 2008~~ March 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	3.1 CalPERS' Data Owners and Custodians Practice states that data owners are responsible for authorizing access to assets. However, it does not clearly state who should authorize logical access by technical support staff, and physical access to locations where Electronic Protected Health Information can be accessed.	IN PROGRESS. The Information Security Office states that it is preparing a new process by which data owners can give Information Technology Services senior management the authority to approve access for technical support staff. Information Technology Services will be required to establish access authorization processes that require two levels of approval. The Information Security Office states that it will revise the Lincoln Plaza Complex Access Card Security Practice to include physical security requirements for the Regional Offices and the Emergency Operations Center. The Information Security Office plans to implement the new process and practice by ~~August 2008~~ March 2009.
		3.2 CalPERS' Data Owners and Custodians Practice is not clear on who should supervise employees and contractors working with Electronic Protected Health Information in areas that are outside the data owner's control. Information Security should establish or modify security practices to provide clearer guidelines.	IN PROGRESS. The Information Security Office states that it has purchased an appliance to assist data owners with monitoring responsibilities. It expects the appliance to be operational by October 2008. The Information Security Office states that it plans to create a HIPAA Security Practice to provide guidelines for supervising employees and contractors working with Electronic Protected Health Information in locations outside the data owner's area of control. The Information Security Office states that the new practice will be drafted after the Health Benefits Branch risk assessment completed in August 2008 and plans to finalize the practice by ~~October 2008~~ March 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued*	Information Security Office	3.6 CalPERS has not performed a risk assessment to determine whether the current extent of employment screening process is sufficient for protecting Electronic Protected Health Information. Information Security, upon completion of risk analysis, should assess whether current screening is sufficient.	IN PROGRESS. The Information Security Office states it requested a legal opinion regarding CalPERS' ability to implement background checks in July 2006; the opinion was delivered on November 9, 2007. The Information Security Office is working with Human Resources on the feasibility of augmenting existing reference check processes. The Information Security Office states that it plans to document any additional security requirements a new HIPAA Security Practice. The Information Security Office states that the new practice will be drafted after the Health Benefits Branch risk assessment completed in August 2008 and plans to finalize the practice by ~~October 2008~~ March 2009.
		3.9 CalPERS does not have a security practice that requires timely termination of physical access to locations where Electronic Protected Health Information can be accessed. Information Security should establish or revise current security practice to define the requirement.	IN PROGRESS. The Information Security Office states it will revise the Lincoln Plaza Complex Access Card Security Practice to include timely termination requirements and extend physical security requirements to the Regional Offices and the Emergency Operations Center. These requirements will be included in the new HIPAA Security Practice. The Information Security Office plans to revise the Lincoln Plaza Complex Access Card Practice by August 2008 and complete the new HIPAA Security Practice by ~~October 2008~~ March 2009.
		4.3 CalPERS' User Account Maintenance Practice requires timely modification of user access; however, it does not contain requirements regarding access establishment. Information Security should modify the practice to provide clearer guidelines.	IN PROGRESS. The Information Security Office states that it has modified the Data Owner and Custodian Practice and published the Identity Authentication Practice. The Information Security Office states it will address data owner responsibilities for Electronic Protected Health Information in the new HIPAA Security Practice which is to be completed in ~~October 2008~~ March 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued*	Information Security Office	5.1 CalPERS' Virus Practice requires anti-virus software to be installed on all applicable computer server systems; however, it does not clearly define which servers are applicable. Information Security should revise the Practice to clarify which servers are required to have the software installed.	IN PROGRESS. The Information Security Office states that it has amended the practice to require all servers to have anti-virus software installed. The Information Security Office, in collaboration with Information Technology Services Branch, purchased compliance tools to ensure servers have the required controls in place. The new HIPAA Security Practice will document controls relied on to guard against, detect and report malicious software. The Information Security Office states that the new HIPAA Security Practice will be completed and revised, if necessary, upon implementation of the compliance tools and that these tools should be fully implemented by ~~December 2008~~ March 2009.
		5.2 CalPERS Event Logs Practice requires logging of invalid user authentication attempts and unauthorized attempts to access resources. Information Security should incorporate current log-in monitoring practices into security risk analysis and risk mitigation strategy.	IN PROGRESS. The Information Security Office states it evaluated processes used to monitor invalid log-in attempts as part of its IT infrastructure risk assessment completed in April 2008. In addition, the Information Security Office has purchased a logging and monitoring tool. The Information Security Office states it is on track with the Health Benefits Branch risk assessment and the new HIPAA Security Practice. However, implementation of the logging and monitoring tool is delayed due to resource constraints. The Information Security Office is working with the Information Technology Services Branch to develop an implementation schedule to install in a test environment and will document event logging requirements specifically for systems that contain Electronic Protected Health Information in a new HIPAA Security Practice to be published in ~~October 2008~~ March 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	5.3 Information Technology Services uses systems to enforce password standards when feasible. Information Security should incorporate various administrators' current password practices into the security risk analysis and risk mitigation strategy.	IN PROGRESS. The Information Security Office will develop and provide password security awareness training for administrators. In addition, it will document deviations from the Identity Authentication Practice as exceptions are discovered during the risk assessment. Target completion date ~~June 2008 August 2008~~ March 2009.
		5.4 Deviations from the CalPERS Password Practice were not always supported with documented variances approved by Information Security. Information Security should ensure that system administrators implement procedures and comply with the Practice.	IN PROGRESS. The Information Security Office will work with system administrators to implement procedures to ensure compliance with CalPERS' Identity Authentication Practice for all information systems containing Electronic Protected Health Information. These requirements will be included in the HIPAA Security Practice. Target completion date is ~~October 2008~~ March 2009.
		6. CalPERS' Information Security Incidents Practice defines the events considered to be reportable incidents; however, current security practice and procedures do not adequately specify response efforts. Information Security should amend current security practices.	IN PROGRESS. The Information Security Office states that the HIPAA Security Practice will define incidents reportable specific to Electronic Protected Health Information and the systems that contain it, and document what must be reported to the Information Security Office. It will also document processes for gathering evidence, eliminating known damage and causes of incidents, and external communication and reporting. The HIPAA Security Practice will be published in ~~October 2008~~ March 2009.
		8.1 CalPERS has not conducted a thorough assessment of potential risks and vulnerabilities to Electronic Protected Health Information security. Information Security should establish security baselines upon completion of a risk analysis.	IN PROGRESS. The Information Security Office states that the risk assessment of the Health Benefits Branch and any other systems containing Electronic Protected Health Information will be used to establish and document security baselines. In addition, the new HIPAA Security Practice will consolidate security requirements specific to protecting Electronic Protected Health Information. The new HIPAA Security Practice will be completed by ~~October 2008~~ March 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	8.2 Information Security should establish a process for periodic evaluation of administrative, physical, and technical safeguards in response to environmental or operational changes affecting the security of Electronic Protected Health Information.	IN PROGRESS. The Information Security Office states that it has implemented the Risk Assessment and Management Program, which consists of a biennial cycle of risk assessment of all program areas and an annual assessment of technology use and infrastructure management. In addition to the Risk Assessment and Management Program, staff will develop procedures to periodically assess compliance with administrative, physical, and technical safeguards for Electronic Protected Health Information. Recommendations for mitigations will be made, and remediation activities will be tracked and monitored. The assessment procedures will be developed in conjunction with the implementation of the monitoring tools by June 2009.
		8.4 CalPERS' Certification and Accreditation Practice requires that information applications and/or systems must undergo security certification and accreditation to certify that the information is protected. Information Security should ensure that this is performed periodically.	IN PROGRESS. The Information Security Office states that it is working with Information Technology Services to revise the certification and accreditation process. The Information Security Office is updating its corrective action plan for this finding. The target completion date is June 2009.
		9.4 The Information Security Office should ensure that CalPERS develops appropriate security requirement provisions to be included in all existing and future business associate contracts.	IN PROGRESS. The Information Security Office has developed new contract language for use with business associate agreements and is in the process of getting approval for the new language. The Information Security Office is updating its corrective action plan for this finding. The target completion date is February 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	10.1 CalPERS currently does not have a security practice that addresses granting facility access during an emergency. Information Security should establish security practices to outline physical security requirements.	IN PROGRESS. The Information Security Office has determined that the best approach to ensure the integrity and confidentiality of information assets during an emergency is to have a single security policy that is applicable in all situations. This approach will be validated when implementing the Risk Assessment and Management Program. Information Security Office will revise security practices to incorporate this approach by ~~August 2008~~ March 2009.
		10.3 Currently, Information Security does not have information security practices addressing physical security. It should establish security practice(s) to specify facility security requirements based on the risk assessment.	IN PROGRESS. The Information Security Office states that upon completion of the Health Benefits Branch risk assessment, it will a new develop a HIPAA Security Practice that will define specific requirements for limiting physical access to the data center, communications closets, and the Emergency Operations Center. In addition, the new practice will address physical security of the environmental controls over the data center and Emergency Operations Center, as well as desktop, laptop and workstation location security. The Health Benefits Branch risk assessment was completed in August 2008. The HIPAA Security Practice will be completed in ~~October 2008~~ March 2009.
		10.5 CalPERS security practices do not require documentation of repairs and modifications to security related physical components of headquarter buildings. Information Security should establish a practice to require documentation.	IN PROGRESS. The Information Security Office states that upon completion of the Health Benefits Branch risk assessment, it will develop new criteria for documenting repairs and modifications to the physical security components. The Information Security Office will document the criteria in the new HIPAA Security Practice to be completed by ~~October 2008~~ March 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	11.1 CalPERS security practices do not specify proper functions to be performed on all different types of workstations, and physical attributes of the surroundings of a specific workstation. Information Security Office should establish these practices.	IN PROGRESS. The Information Security Office states that it has modified security practices to specify physical attributes of workstations based on its knowledge of how Electronic Protection Health Information can be accessed at CalPERS. It conducted a security risk assessment of the Health Benefits Branch completed in August 2008. Any mitigation measures identified will be included in the new HIPAA Security Practice to be completed by ~~October 2008~~ March 2009.
		12. Because workstations are located in areas where physical access is more permissive than logical access, physical access alone does not restrict workstation access to only authorized users of Electronic Protected Health Information. Information Security should incorporate this as part of the risk analysis.	IN PROGRESS. The Information Security Office states that the Health Benefits Branch risk assessment will incorporate current workstation security as part of the risk analysis and evaluate the need for increased physical security for workstations, particularly those outside of Health Benefits Branch, or increased used of alternative logical access safeguards to ensure adequate workstation security. These requirements will be incorporated into the HIPAA Security Practice to be completed by ~~October 2008~~ March 2009.
		13.2 Information Security practices do not specifically address media re-use. Media may include removable diskettes used by employees. Information Security Office should either amend the practices to specifically address media re-use or establish an additional practice.	IN PROGRESS. The Information Security Office hired two new staff in April 2008. The target date to commence compliance visits has been delayed to ~~August 2008~~ September 2009. The Information Security Office is updating its corrective action plan for this finding.
		13.4 CalPERS' security practices do not specifically require the maintenance of records tracking the movements of hardware and electronic media internally. Information Security should determine if this is necessary and then establish or amend security practices as necessary.	IN PROGRESS. The Information Security Office states that IT infrastructure risk assessment is complete but has not finished management review. Upon management review, the identified mitigations will be undertaken. The Information Security Office is updating its corrective action plan for this finding. The target completion date is March 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	**Responsibility**	**Description of Risk / Finding**	**Status/Comments**
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	13.6 Current security practices and procedures do not require data backup to be created prior to moving equipment. Information security should address the need to require data to be backed up before movement of equipment.	IN PROGRESS. The Information Security Office is updating its corrective action plan for this finding. The target completion date is March 2009.
		14.1 Technical support staff using shared accounts to access systems that maintain Electronic Protected Health Information do not always obtain an approved variance. Information Security should notify Security Administration upon identification of all systems containing Electronic Protected Health Information.	IN PROGRESS. The Information Security Office states that the assessment of Health Benefit Branch is scheduled for March 2008 to May 2008. Applications used by Health Benefits Branch will be identified and all access will be mapped. The Information Security Office is updating its corrective action plan for this finding. The target completion date is June 2009.
		14.3 CalPERS does not have a security practice that addresses access control during an emergency. Information Security should set forth security requirements that access should be restricted only to those persons that have been granted access rights during an emergency.	IN PROGRESS. The Information Security Office states that all provisions and requirements defined in the security practices apply in all situations, including emergencies, and a revised policy clearly stating this will be published. The Information Security Office is updating its corrective action plan for this finding. The target completion date is March 2009.
		14.6 CalPERS does not require any data, including Electronic Protected Health Information, to be encrypted when sent across internal networks and while in storage. Information Security should address this need based on risk analysis results.	IN PROGRESS. The Information Security Office has conducted an IT infrastructure risk assessment and will consider whether it is necessary to require encryption of data at-rest and in-motion on internal CalPERS-controlled networks. If yes, additional resources will be identified and funds will be requested through the budget request process. The Information Security Office is updating its corrective action plan for this finding. The target completion date is June 2009.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	**Responsibility**	**Description of Risk / Finding**	**Status/Comments**
HIPAA Security Compliance Review (10/20/06) *(continued)*	Information Security Office	15.1 CalPERS' Event Logs Practice does not require a retention period of 6 years or recording of functions performed. Information Security should modify the Event Logs Practice to require the recording and retention requirements.	IN PROGRESS. The Information Security Office is revising the event logs requirement. The Information Security Office purchased an event logging appliance in May 2007. This tool is capable of collecting logs in such a manner that impact on system performance is expected to be minimal. The Information Security Office is updating its corrective action plan for this finding. The target completion date is June 2010.
		15.2 The Document Management System does not log who viewed imaged documents, or when and where the imaged documents are created, printed, exported, or viewed. The Event Logs Practice should be modified to provide clearer guidelines.	IN PROGRESS. The Information Security Office is revising the event logs requirement. The Information Security Office purchased an event logging appliance in May 2007. This tool is capable of collecting logs in such a manner that impact on system performance is expected to be minimal. The Information Security Office is updating its corrective action plan for this finding. The target completion date is June 2010.
		16. A thorough risk analysis of the technical environment in which all Electronic Protected Health Information resides has not been conducted. Upon completion of risk analysis, Information Security should document the controls utilized to corroborate that Electronic Protected Health Information has not been altered or destroyed in an unauthorized manner.	IN PROGRESS. The Information Security Office has conducted the IT infrastructure risk assessment and will document existing security controls and deficiencies. Additional resources may be required to implement remediation. The Information Security Office is updating its corrective action plan for this finding. The target completion date is June 2010.
		18. Because CalPERS has not identified all the locations where Electronic Protected Health Information resides, we cannot determine whether current security measures are adequate. Information Security should determine whether additional controls are needed to ensure that Electronic Protected Health Information is properly protected during transmission.	IN PROGRESS. The Information Security Office has conducted an IT infrastructure risk assessment and will consider whether it is necessary to require encryption of data during transmission. Should additional encryption technology be required, it would be requested as part of the formal budget request process. The Information Security Office is updating its corrective action plan for this finding. The target completion date is June 2010.

AGENDA ITEM 5
SPECIAL UPDATE ON HIPAA AUDIT RESOLUTION STATUS
AS OF DECEMBER 31, 2008

Audit Activity (Report Issue Date)	Responsibility	Description of Risk / Finding	Status/Comments
HIPAA Security Compliance Review (10/20/06) *(continued)*	Security Administration	8.3 Security Administration should ensure timely implementation of technical safeguards once the security baselines are established and updated.	IN PROGRESS. Security Administration Services, in coordination with the Information Security Office and Office of Audit Services, has made progress in developing the Certification and Accreditation process. Once all systems containing HIPAA data are identified by the Information Security Office, Security Administration will schedule those systems for the certification process. A corrective action plan was submitted. The target completion date is pending Information Security Office's identification of all systems containing HIPAA data.
		13.5 Information Technology Services does not maintain an inventory policy for devices and electronic media. Upon Information Security's completion of security practice regarding tracking of hardware and electronic media, it should amend its policy manual to ensure compliance.	IN PROGRESS. Information Technology Services Security Administration states that once the Information Security Office completes its risk assessment and security practices regarding tracking of hardware and electronic media, Information Technology Services will amend its policy manual to ensure compliance. A corrective action plan was submitted; the target completion date is pending completion of tasks by the Information Security Office.
		14.2 Technical support staff using shared accounts to access systems that maintain Electronic Protected Health Information do not always obtain an approved variance. Security Administration should ensure that all users have a unique identifier. An approved variance should be obtained and documented for all shared IDs.	IN PROGRESS. As systems containing electronic protected health information are identified by the Information Security Office during its IT infrastructure risk assessment, Security Administration will follow up to resolve the issue. To eliminate future problems with shared accounts, Security Administration has changed procedures to reject all requests of a shared account without an approval from the Information Security Office. The target completion date is pending Information Security Office's identification of all systems containing HIPAA data.